UNITED STATES PATENT AND TRADEMARK OFFICE

nl

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/046,496	10/29/2001	Carey Nachenberg	20423-05957	3384

34415 7590 10/03/2007

SYMANTEC/ FENWICK
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER	
WILLIAMS, JEFFERY L	

ART UNIT	PAPER NUMBER
2137	

NOTIFICATION DATE	DELIVERY MODE
10/03/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptoc@fenwick.com
bhoffman@fenwick.com
aprice@fenwick.com

Office Action Summary	**Application No.** 10/046,496	**Applicant(s)** NACHENBERG ET AL.
	Examiner Jeffery Williams	**Art Unit** 2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 25 July 2007.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-17,20 and 22-33 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-17,20 and 22-33 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 7/25/07.
4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application
6) □ Other: _____.

DETAILED ACTION

This action is in response to the communication filed on 7/25/07.

All objections and rejections not set forth below have been withdrawn.

Claims 1 – 17, 20, 22 – 33 are pending.

Specification

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Claim 8 recites added language "the computer code *is determined to be executable only* when the computer code is time stamped…" The specification fails to provide proper antecedent basis for this recitations.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 8 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Applicant has not pointed out where the new (or amended) claim is supported, nor does there appear to be a written description of the claim limitations in the application as filed (see above objection to the specification).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 – 10 and 12 – 33 rejected under 35 U.S.C. 103(a) as being unpatentable over Bates et al. (Bates), U.S. Patent 6,721,721 B1 in view of Hericourt et al. (Hericourt), U.S. Patent 7,099,916.

Regarding claim 1, Bates et al. discloses:

entering a first computer virus status mode in response to a first computer virus outbreak report indicating a virus attack threat to a computer network (Bates et al., col. 1, lines 13-52). Bates et al. reports the outbreak of new and more sophisticated viruses, and in response, the system of Bates et al. is employed for the purpose of protecting against these outbreaks.

computing a first computer virus alert time corresponding to entry into the first computer virus status mode (Bates et al., fig. 7, elem. 214; col. 7, lines 20-35). Herein, Bates et al. discloses a method for accessing computer content on a local machine or on a network. Content is filtered based upon a generated virus alert time, a rule derived from relative time parameters (criterion) entered (via computer means, "computing") by a user in a virus status mode. The relative time parameters (i.e. "virus found in last 7 days", "not checked in last 14 days") are processed ("computing") into a rule, which is then utilized by the system to compare with the timestamps of content and make determinations of trustworthiness (Bates et al., col. 11, lines 12-24; col. 13, lines 22-34; col. 17, lines 35-49; col. 18, lines 22-30).

comparing a time stamp of a executable computer code with the first computer virus alert time (Bates et al., col. 9, line 65 – col. 10, line 3; col. 11, lines 12-24; col. 12, lines 59-62);

and determining the executability of the computer content in response to the result of the comparing step (Bates et al., col. 9, line 56 – col. 10, line 8; col. 11, lines 12-24). Bates et al. discloses that in response to a comparison, a determination of computer content executability is performed.

Bates discloses that a time stamp of the executable code corresponds, *inter alia*, to the time the code was virus scanned. However, Bates does not explicitly disclose that a time stamp of the executable computer code corresponds to an execution time of the computer code.

Hericourt teaches that virus scanning of executable code comprises an execution of the code, and therefore "an earliest moment" the code is allowed to execute (3:25-54).

It would have been obvious to one of ordinary skill in the art to recognize teachings of Hericourt within the system of Bates. This would have been obvious because one of ordinary skill in the art would have been motivated by the general teachings of Bates for virus scanning and the teachings of Hericourt for the effective accomplishment of such.

Regarding claim 2, the combination enables:

receiving a first access control time based on the first virus outbreak report (Bates et al., fig. 7, elem. 214). The system of Bates et al. takes human input and "automatically" generates computer readable parameters.

and converting the first access control time into the first virus alert time (Bates et al., fig. 7, elem. 214; col. 12, lines 59-62). A "prior point in time" ("virus alert time") is derived from the period of time specified by element 214 ("access control time") and is compared to the timestamp of the file.

Regarding claim 3, the combination enables:

wherein the first access control time is a relative time stamp (Bates et al., fig. 7, elem. 214; col. 12, lines 59-62). A “prior point in time” (“virus alert time”) is derived from the period of time specified by element 214 (“access control time”) and is relative in time.

Regarding claim 4, the combination enables:

wherein the first access control time is a pre-determined time period for access control under the first computer virus status mode (Bates et al., fig. 7, elem. 214). The access control time is pre-determined by the user.

Regarding claim 5, the combination enables:

determining the presence of a value representing the computer content in a memory table of executable computer content (Bates et al., col. 7, lines 12-34).

Regarding claim 6, the combination enables:

wherein the computer content is not executed when the value representing the computer content is not present in the memory table of executable computer content (Bates et al., col. 11, lines 11-24; col. 3, lines 24-27). As disclosed by Bates et al., content not present in the memory table of executable computer content is flagged as untrustworthy. The invention as disclosed by Bates et al. is configurable to eliminate untrustworthy computer content from the list of accessible content, thus not providing access to the content for execution.

Regarding claim 7, the combination enables:

wherein the value is a hash value of the computer content (Bates et al., col. 12, lines 55-58).

Regarding claim 8, the combination enables:

wherein the computer content is determined to be executable only when the computer content is time stamped prior to the first computer virus alert time (Bates et al., col. 13, lines 42-59; col. 3, lines 24-27). Computer content that is time stamped prior to the first computer virus alert time is branded as trustworthy. Thus, the content would not be subjected to denial of access for execution.

Regarding claim 9, the combination enables:

entering types of computer codes that should be blocked from execution in response to the first computer virus outbreak report (Bates et al., col. 9, line 62 – col. 10, line 28);

and blocking execution of a computer code that belongs to the entered types of computer codes (Bates et al., col. 3, lines 24-27). The invention as disclosed by the combination is configurable to eliminate untrustworthy computer content from the list of accessible content, thus not providing access to the content for execution.

Regarding claim 10, the combination enables:

generating a second virus alert time in response to a second computer virus outbreak report; comparing the time stamp of the computer content with the second computer virus alert time; determining the executability of the computer content in response to the result of comparing the time stamp of the computer content with the second computer virus alert time (Bates et al., col. 3, lines 5 – 15). The above limitations of claim 10 are essentially similar to claim 1 with the exception that they are directed to a second instance of the method of claim 1. The combination enables for the method of claim 1 produces a set of results. Thus, the combination enables a secondary instance of the method of claim 1, as a the word "set" dictates more than a singular occurrence of the method of claim 1.

performing antivirus processing upon the computer content (Bates et al., col. 9, lines 62-66). The combination enables the processing of computer content for the likelihood of existing viruses.

Regarding claim 12, it is rejected, at least, for the same reasons as claim 1, and furthermore because the combination enables:

an access control console, for entering a first computer virus status mode in response to receiving a computer virus outbreak report indicating a virus attack threat to a computer network and for recovering a preselected virus access control time corresponding to said virus status mode (Bates et al., fig. 1, elem. 33; fig. 7);

an anti-virus module, coupled to the access control console, configured to compute a virus alert time based on the virus access control time and to compare a time *stamp of target computer code corresponding to an earliest moment the computer code was allowed to execute with the virus alert time prior to execution of the target computer content* (Bates et al., fig. 1, elem. 30; see rejections of claims 1 and 2).

and wherein the anti-virus module is further configured to determine the executability of the computer content in response to comparing the time stamp of the target computer content with the virus alert time (Bates et al., col. 9, line 56 – col. 10, line 8; col. 11, lines 12-24). The combination enables for in response to a comparison, a determination of computer content executability is performed. Thus the combination enables *content executability determination,* comprising an *anti-virus module*, used to determine the trustworthiness ("executability") of content.

Regarding claim 13, the combination enables:

a memory module for storing time stamps of the plurality of computer contents (Bates et al., fig. 1, elem. 46);

and an access control module, coupled to the access control console and to the memory module, for computing the virus alert time and for comparing the time stamp of each target computer content with the virus alert time (Bates et al., fig. 1, elem. 42; see rejections of claims 1 and 2).

Regarding claim 14, the combination enables:

a computer virus processing module, coupled to the access control module, for further processing a target computer content in order to determine the executability of the target computer content (Bates et al., fig. 1, elem. 44).

Regarding claim 15, the combination enables:

wherein the memory module stores a value representing each of the computer contents (Bates et al., col. 12, lines 52-65).

Regarding claim 16, the combination enables:

wherein the access control module is configured to determine the presence of the value in the memory module as representing a target computer content (Bates et al., fig. 3).

Regarding claim 17, the combination enables:

wherein the value is a hash value (Bates et al., col. 12, lines 52-65).

Regarding claim 20, it is rejected, at least, for the same reasons as claim 1, and furthermore because the combination enables:

creating a list of time-stamped executable computer contents (Bates et al., fig. 3, elem. 92).

entering a virus alert mode in response to a virus outbreak report indicating a virus attack threat to a computer network (Bates et al., fig. 2; col. 1, lines 13-52).

responsive to the virus alert mode, entering an access control message for specifying an access control rule for blocking the execution of suspicious or susceptible computer contents that have a time stamp corresponding to an earliest moment the computer file was allowed to execute, and the time-stamp is not before a computed virus alert time, the access control message including a first control parameter for computing the virus alert time (Bates et al., fig. 2; fig. 7; see rejections of claims 1 and 2).

receiving a request to execute a target computer content; and determining the executability of the target computer content based on the access control rule in the access control message (Bates et al., fig. 2).

Regarding claim 22, the combination enables:

receiving the access control message; automatically converting the first control parameter into the virus alert time; comparing the time stamp of the target computer content in the list with the virus alert time; and determining the executability of the target computer content based on the result of the comparing step (Bates et al., fig. 2, fig. 3, fig. 7; see rejections of claims 1 and 2).

Regarding claim 23, the combination enables:

applying an anti-virus operation upon the target computer content (Bates et al., fig. 3).

Regarding claim 24, the combination enables:

a second control parameter for specifying types of computer contents that should be subject to the access control rule (Bates et al., col. 9, line 62 – col. 10, line 28);

a third control parameter for specifying an expiration time for the access control rule (Bates et al., fig. 7, elem. 217);

and a fourth control parameter for identifying the access control message (Bates et al., fig. 2).

Regarding claim 25, the combination enables:

determining validity of the access control message based on the third control parameter (Bates et al., fig. 3);

Regarding claim 26, the combination enables:

determining executability of the target computer content based on the second control parameter (Bates et al., col. 9, line 62 – col. 10, line 28);

.

Regarding claims 27 and 28, they are rejected for the same reasons as claims 20 and 22, and further because the combination enables the usage of their system in a network of communicating computers (Bates et al., fig. 1). Communications to a user can be blocked when computer content is deemed to be untrustworthy (Bates et al., col. 3, lines 24-27, col. 14, line 6 – col. 15, line 8).

Regarding claim 29, the combination enables:

wherein the data communication is blocked when the target computer content is time-stamped not before the virus alert time (Bates et al., fig. 3; fig 7).

Regarding claim 30, it is rejected, at least, for the same reasons as claim 1, and furthermore because the combination enables:

a firewall module monitoring data communications initiated by a target computer content and sending a request to examine the data communications (Bates et al., fig. 1, elems.20, 30, 50). The combination enables that the system is useful in a network and it is capable of filtering trustworthy and untrustworthy computer content – thus, acting as a firewall module.

an access control console, for generating an access control message specifying an access control rule for blocking data communications of the target executable computer file that has a time stamp corresponding to an earliest moment the computer file was allowed to execute, and the time-stamp is not before a virus alert time, the access control message including a first control parameter for computing the virus alert time in response to a virus outbreak report indicating a virus attack threat to a computer network (Bates et al., fig. 7; fig. 2);

and an access control module, coupled to the access control console and the firewall module, configured to receive the access control message and a request from the firewall module, and to compute the virus alert time based on the virus access control time and to determine whether the data communication should be blocked *based on the access control rule* (Bates et al., fig. 1, elem. 44, see rejections of claims 1 and 2).

Regarding claim 31, it is a program and computer medium claim implementing the method claim 1, and it is rejected for the same reasons (see also, Bates et al., fig. 1).

Regarding claim 32, it is rejected, at least, for the same reasons as claim 1, and furthermore because the combination enables:

means for entering a computer virus status mode in response to a virus outbreak report indicating a virus attack threat to a computer network and for automatically recovering a preselected virus access control time (Bates et al., fig. 7);

coupled to the entering and recovering means, means for computing a virus alert time based on the virus access control time (Bates et al., fig. 1, elems. 31, 42, 44),

and coupled to the computing virus alert time means, means for comparing a time stamp of a target computer content with the virus alert time prior to execution of the computer content (Bates et al., fig. 1, elem. 42),

and for determining the executability of the computer content in response to comparing the time stamp of the target computer content with the virus alert time (Bates et al., col. 9, line 56 – col. 10, line 8; col. 11, lines 12-24). The combination enables a determination of computer content executability is performed for determining the trustworthiness ("executability") of content.

Regarding claim 33, it is rejected, at least, for the same reasons as claim 1, and furthermore because The combination enables:

means for storing time-stamped executable computer contents (Bates et al., fig. 1, elem. 46);

a firewall means for monitoring data communications occurring to the executable computer contents (Bates et al., fig. 1, elems. 44, 29, 52).

means for entering a computer virus status mode in response to a virus outbreak report indicating a virus attack threat to a computer network and for automatically recovering a preselected virus access control time (Bates et al., fig. 7);

coupled to the entering and recovering means, means for computing a virus alert time based on the virus access control time *(Bates et al., fig. 1, elems. 31, 42, 44).*

and coupled to the computing virus alert time means, the storing means, and the firewall means, means for comparing a time stamp of an executable computer content with the virus alert time to determine whether the data communication occurring to the executable computer content should be blocked (Bates et al., fig. 1, elem. 44, 42).

Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Bates et al. and Hericourt in view of Symantec, "Norton AntiVirus Corporate Edition".

Regarding claim 11, The combination enables that viruses can be found in email attachments, and that it is well known in the art for antivirus programs to have the capability for performing antivirus processing on emails and email attachments (Bates et al., col. 1, lines 35-63). The combination enables an antivirus program or module for performing such antivirus processing (Bates et al., fig. 1, elems. 44, 52). Bates et al., however, does not disclose the details of the antivirus processing for emails and email attachments. Specifically, Bates et al. does not disclose that the antivirus program or module removes the computer content from the E-mail body, and denies execution of the computer content.

Symantec discloses an antivirus program and the details of how the program performs antivirus processing upon an email with an attachment. Symantec discloses that the antivirus program scans content attached to an email body and removes such content if it is found to contain a virus, thus, denying execution of the content (Symantec, page 15, par. 2; page 22, “Managing Realtime Protection”).

It would have been obvious for one of ordinary skill in the art to combine the details disclosed by Symantec for the antivirus processing of emails with the system of Bates et al. because the system of The combination enables an antivirus program capable of performing antivirus processing for processing of emails.

Response to Arguments

Applicant's arguments filed 7/25/07 have been fully considered but they are not persuasive.

Applicants argues or asserts primarily that:

(i) *Assuming that scanning and execution are equivalent (a point Applicants do not concede), neither Bates nor Hericourt discloses or suggests using a time stamp that corresponds to the earliest moment the computer code was allowed to execute. Both references assume that code is scanned multiple times, and neither reference attaches any special significance to the earliest time that the code was scanned (or executed).* (Remarks, pg. 13)

In response, the examiner respectfully points out that the examiner did not assert an equivalency of scanning and execution. However, the examiner does point out (as shown in the rejection of claim 1) that the combination enables for scanning to comprise execution.

Furthermore, it is respectfully noted, in response to applicant's argument that the references fail to show certain features of applicant's invention, that the features upon which applicant relies (i.e., ***the*** *earliest moment the computer code was allowed to execute* and [attaching] *special significance to the earliest time that the code was ... executed...*) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

See Notice of References Cited.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffery Williams
AU: 2137
JW

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER